RSAC 2025 Conference

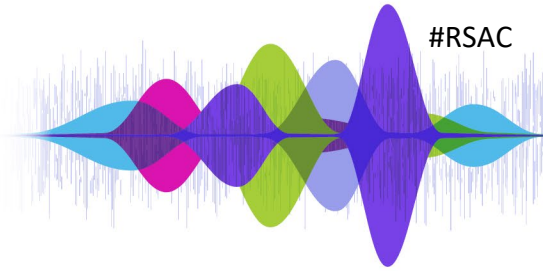
Many Voices.
One Community.

SESSION ID: SAT-R05

Lessons Learned From Implementing an Intel-Based Purple Teaming Process

Carlos Gonçalves

CTI Leader
Banco do Brasil
@carlosecg



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The views and opinions expressed in this presentation are solely my own and do not necessarily reflect those of my employer or any affiliated entities.

RSAC 2025 Conference

Safety Controls are Everywhere

Even if you don’t realize it...

Many Voices.
One Community.

Vehicle Safety

Vehicle Safety

Statistics

- 56% lower fatality risk compared to the late 1950s.
- In total, over 600,000 lives saved.

Source: NHTSA (National Highway Traffic Safety Administration)

Vehicle Safety

Vehicle Safety

Air Bags and Seat Belts

- 50,457 estimated lives saved by frontal air bags from 1987 to 2017.
- 14,955 lives saved by seat belts in 2017.
  - 2,549 additional lives could be saved.

Source: NHTSA (National Highway Traffic Safety Administration)

Improving Vehicle Safety

Old Version

New Version

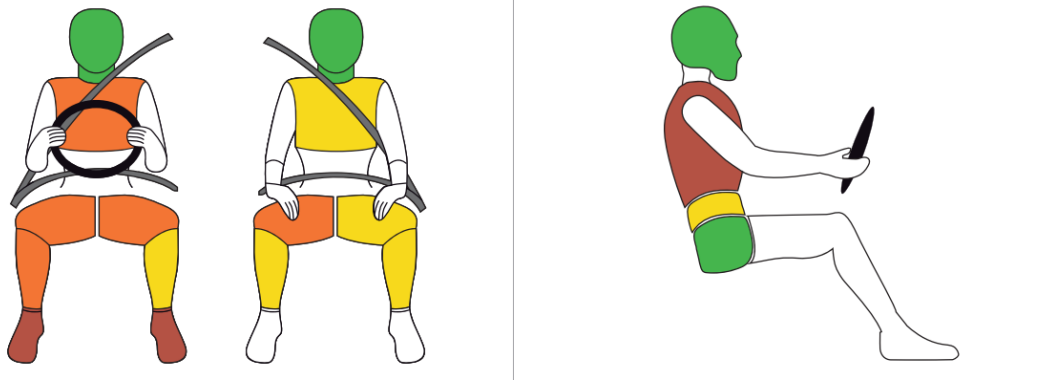
Improving Vehicle Safety

Old Version

22.22 max. 34.00 Adult

24.45 max. 49.00 Child

Frontal offset deformable barrier test 9.318 p	Side movable deformable barrier test (car) 11.903 p

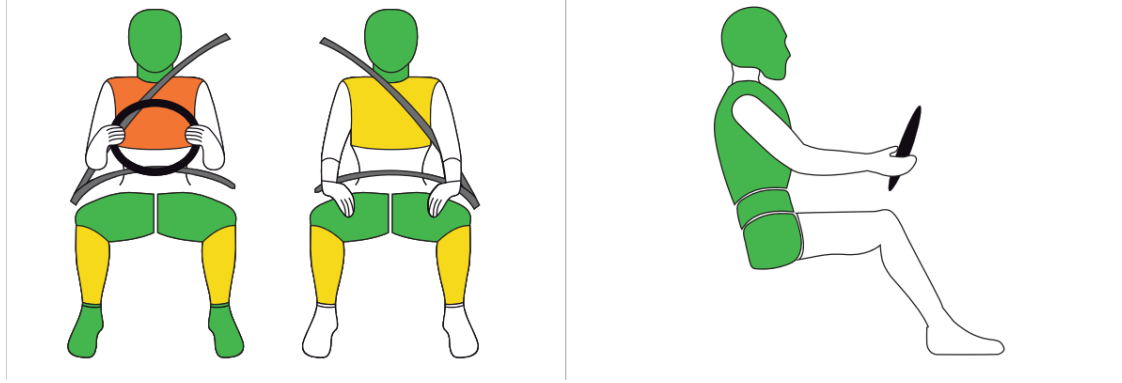


New Version

31.24 max. 34.00 Adult

39.20 max. 49.00 Child

Frontal offset deformable barrier test 13.239 p	Side movable deformable barrier test (car) 16.000 p

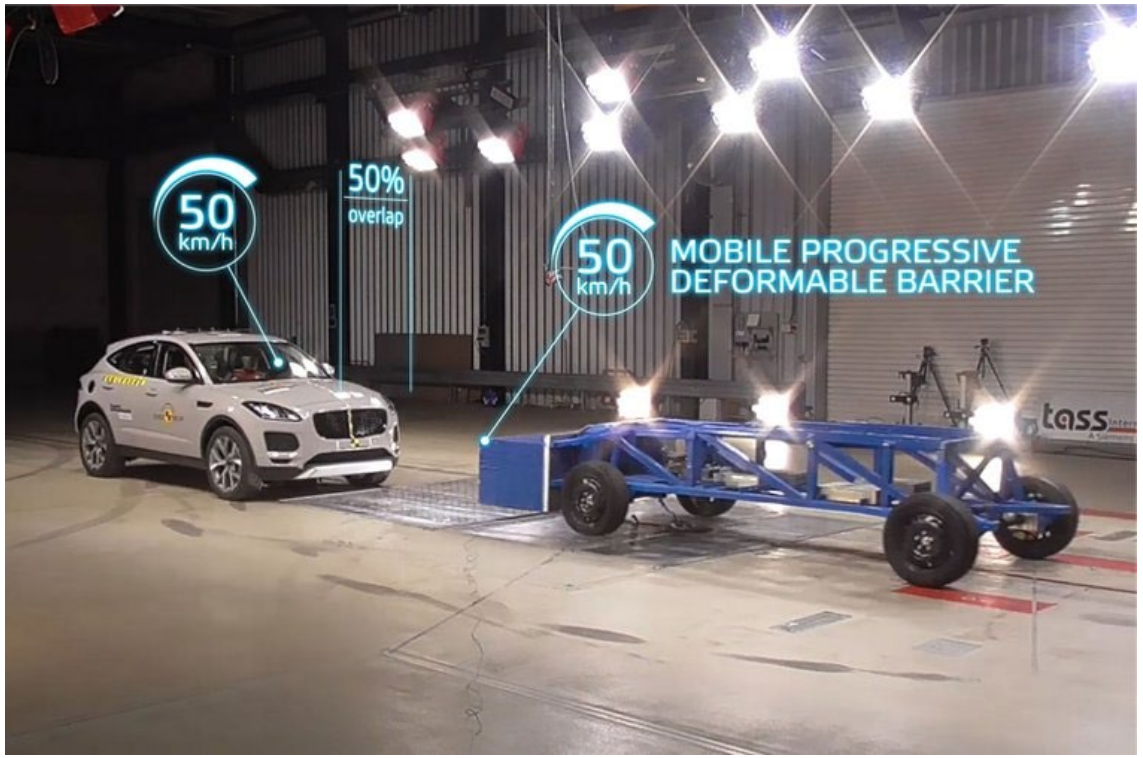


GOOD ADEQUATE MARGINAL WEAK POOR

Crash Test Improvement

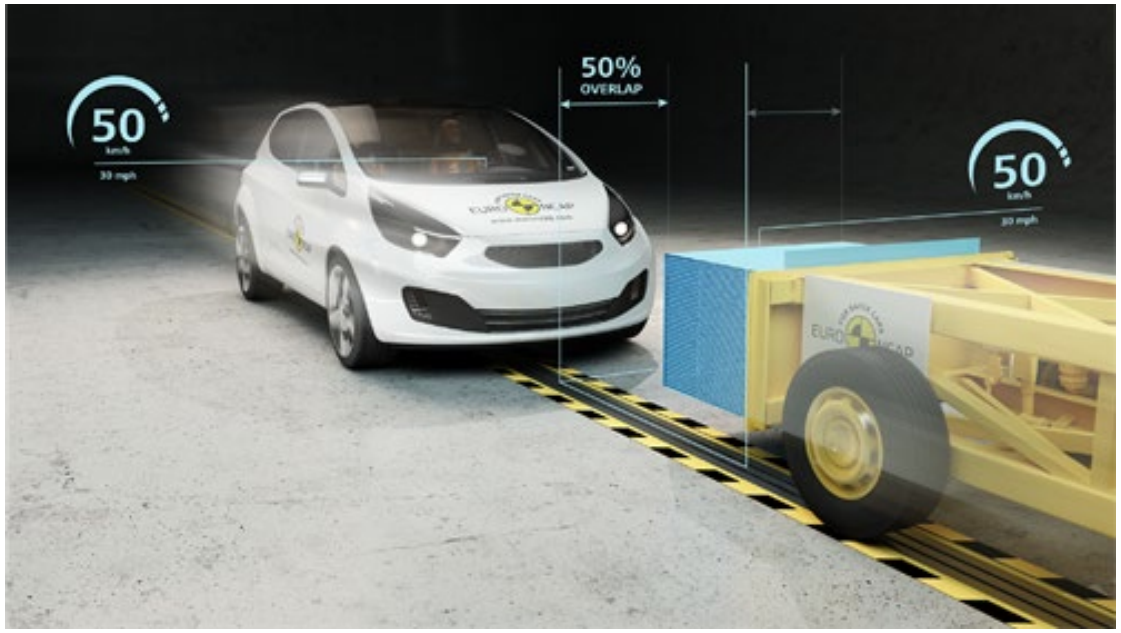
Static Barrier

Moving Barrier



Crash Test Improvement

Mobile Progressive Deformable Barrier



- **Frontal crashes were responsible for more deaths and serious injuries than any other accident type.**
- In most head-on collisions, only a part of the vehicle front width structure is involved.
- Accident data suggest that moderate offsets were most common in Europe.

In summary

- Simulate incidents
- Improve safety mechanisms
- Use real-world incidents knowledge to improve testing procedures
  - Leading to more realistic testing scenarios

RSAC 2025 Conference

Traditional Red/Blue/Purple Teaming

Many Voices.
One Community.

Purple teaming shouldn’t be a wrestle

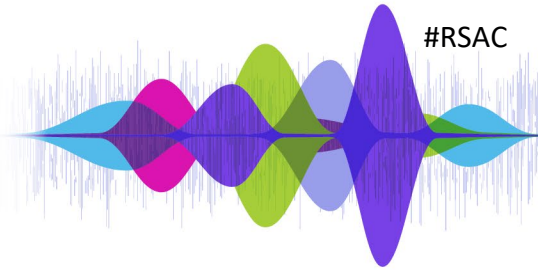
Red and Blue must be in sync

But are they bringing value?

RSAC 2025 Conference

Bringing Intelligence Into the Game

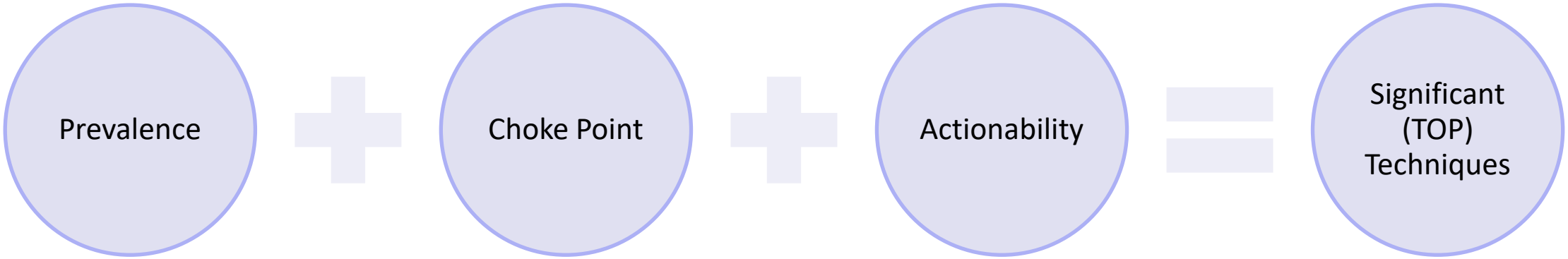
Mitre ATT&CK – Enterprise Tactics

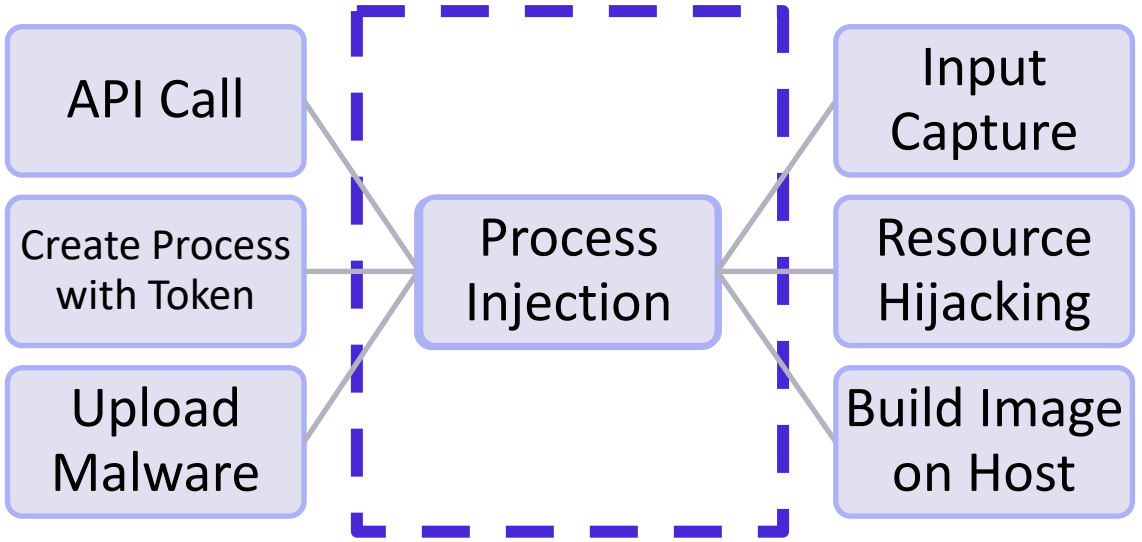


- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

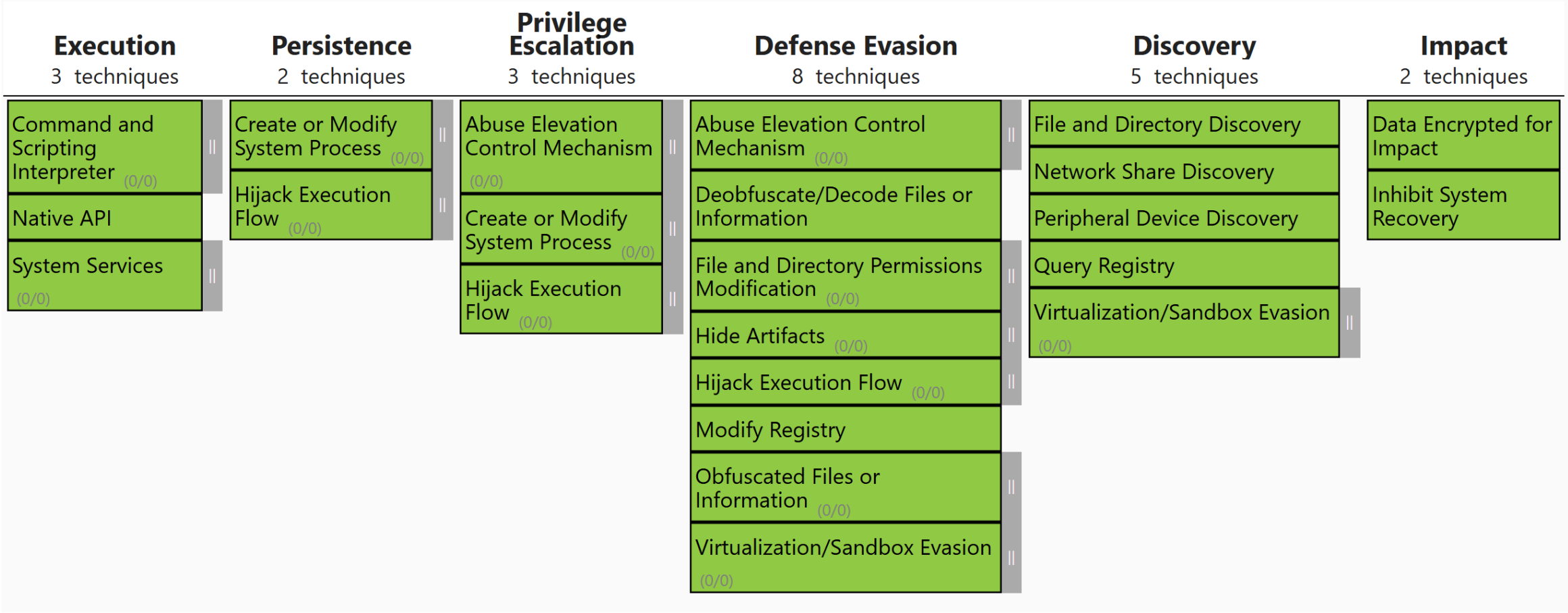
Mitre ATT&CK Enterprise Matrix

Top ATT&CK Techniques

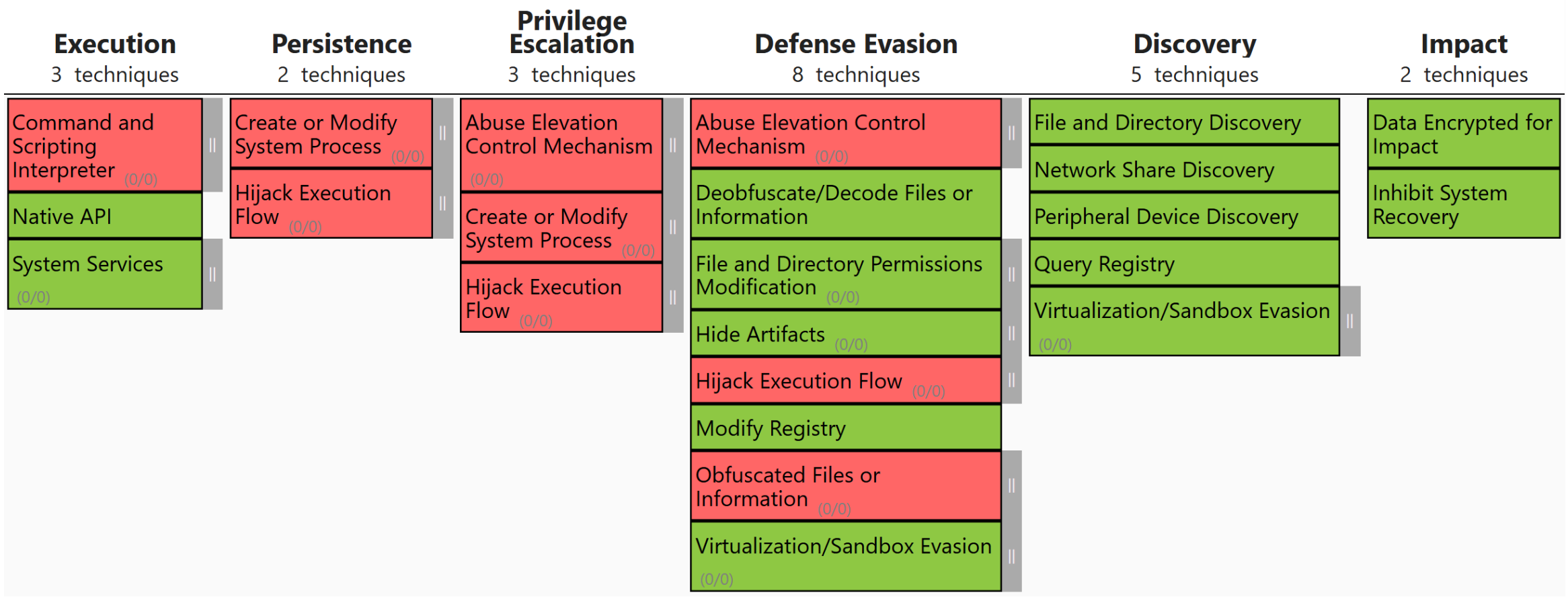




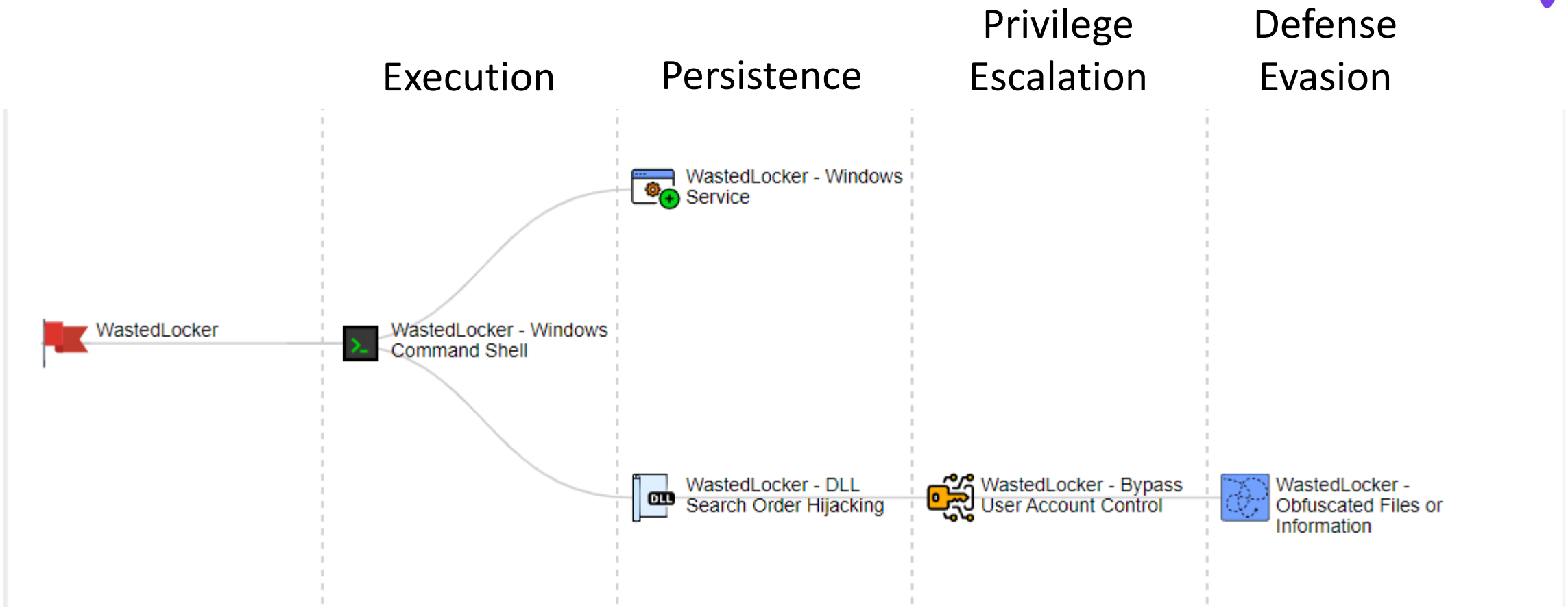
Case Study – WastedLocker Malware



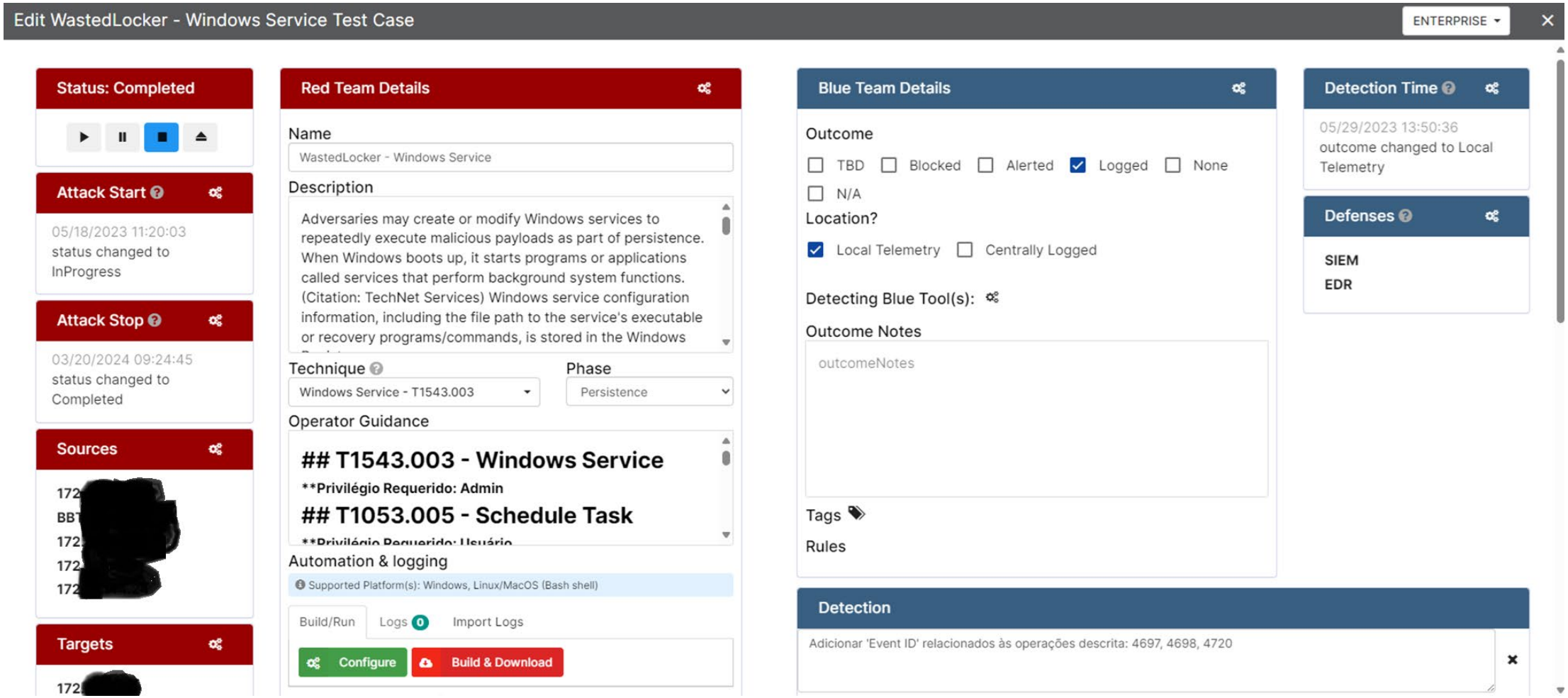
Top Techniques for WastedLocker



WastedLocker Attack Path



Test Case

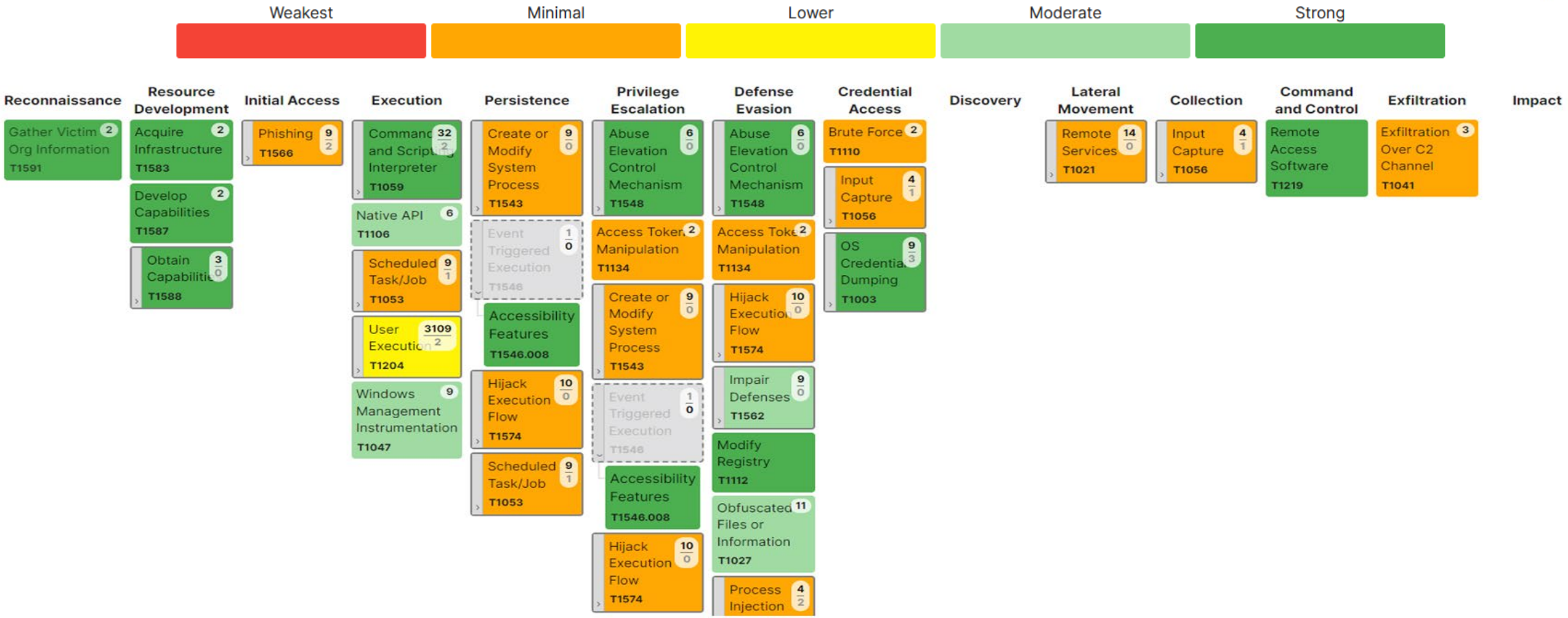

Edit WastedLocker - Windows Service Test Case
ENTERPRISE
Status: Completed
Attack Start
05/18/2023 11:20:03
status changed to InProgress
Attack Stop
03/20/2024 09:24:45
status changed to Completed
Sources
Targets
Red Team Details
Name
WastedLocker - Windows Service
Description
Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions. (Citation: TechNet Services) Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows
Technique
Windows Service - T1543.003
Phase
Persistence
Operator Guidance
T1543.003 - Windows Service
**Privilégio Requerido: Admin
T1053.005 - Schedule Task
Automation & logging
Supported Platform(s): Windows, Linux/MacOS (Bash shell)
Build/Run
Logs 0
Import Logs
Configure
Build & Download
Blue Team Details
Outcome
TBD
Blocked
Alerted
Logged
None
N/A
Location?
Local Telemetry
Centrally Logged
Detecting Blue Tool(s):
Outcome Notes
outcomeNotes
Tags
Rules
Detection Time
05/29/2023 13:50:36
outcome changed to Local Telemetry
Defenses
SIEM
EDR
Detection
Adicionar 'Event ID' relacionados às operações descrita: 4697, 4698, 4720

Defense Capability by Technique

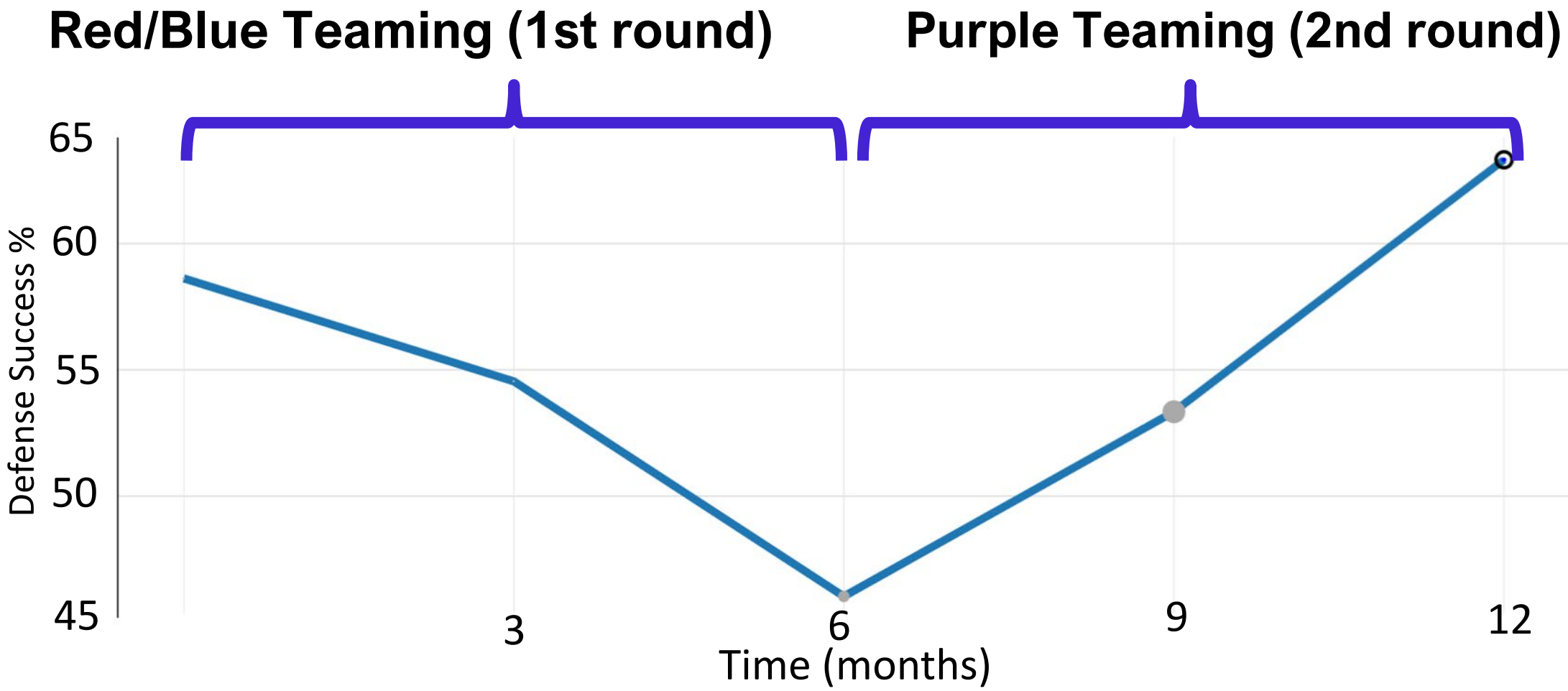
Let’s work together

- Red team’s actions must be in sync with blue team’s
- Detection engineering should be part of the purple team exercises
- Bridge the gap: red + blue + intel for detection engineering

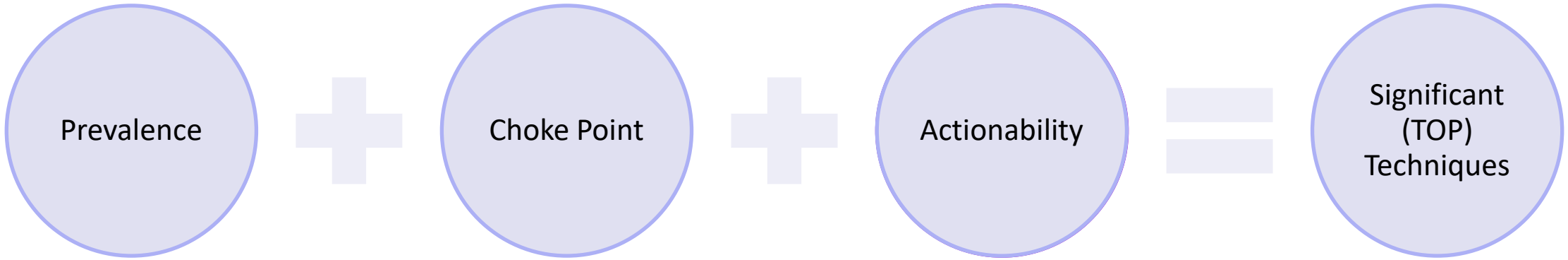
Defense Capability by Technique



Defense Success Rate



Top ATT&CK Techniques

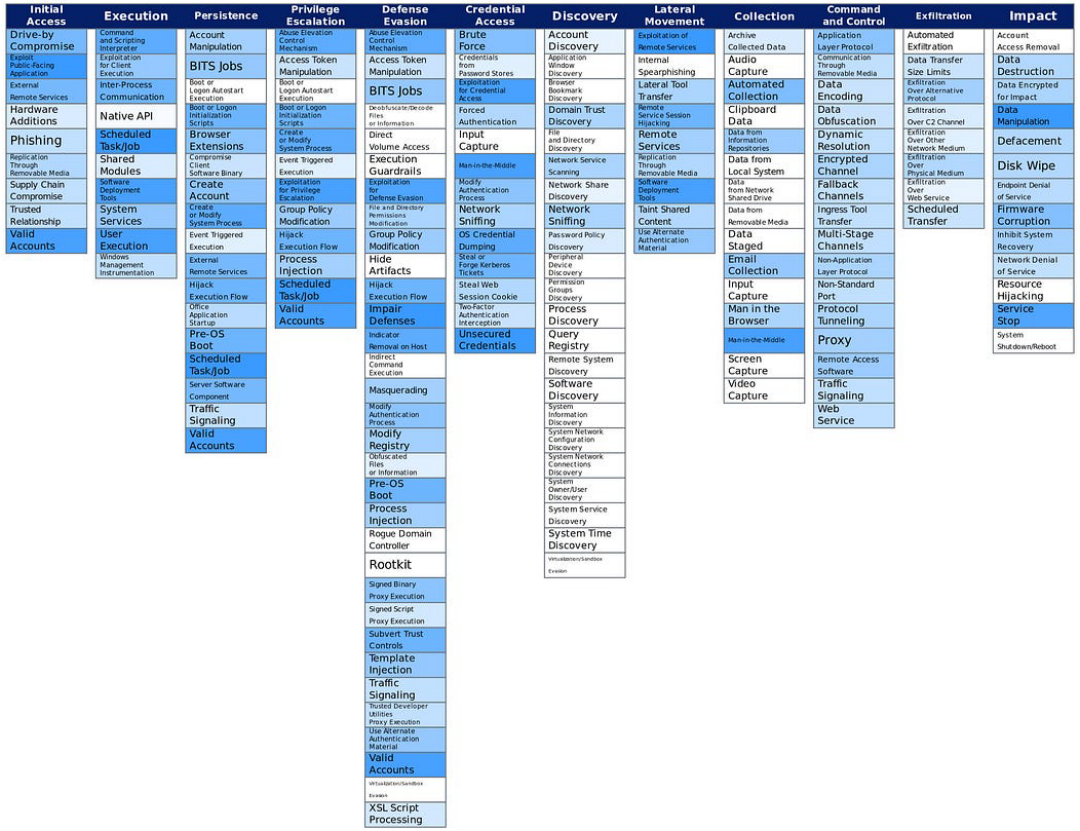


RSAC™ 2025 Conference

Bringing risk to the game

Intel Team Risk Team

Mitre's Mapping Explorer



NIST 800-53

- Mapping of NIST 800-53's controls to ATT&CK's techniques
- Coverage against real-world threats
- Integrate ATT&CK-based threat information into the risk management process.

NIST 800-53 to ATT&CK

Risk Team

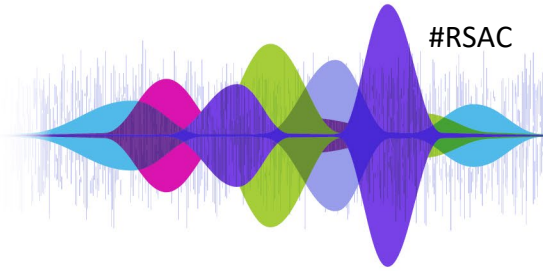
Technical Team

Capability ID	Capability Description	Mapping Type	ATT&CK ID	ATT&CK Name
AC-04	Information Flow Enforcement	Protects	T1001	Data Obfuscation
CA-07	Continuous Monitoring	Protects	T1001	Data Obfuscation
CM-02	Baseline Configuration	Protects	T1001	Data Obfuscation
CM-06	Configuration Settings	Protects	T1001	Data Obfuscation
SC-07	Boundary Protection	Protects	T1001	Data Obfuscation
SI-03	Malicious Code Protection	Protects	T1001	Data Obfuscation
SI-04	System Monitoring	Protects	T1001	Data Obfuscation
AC-04	Information Flow Enforcement	Protects	T1001.001	Junk Data
CA-07	Continuous Monitoring	Protects	T1001.001	Junk Data
CM-02	Baseline Configuration	Protects	T1001.001	Junk Data

Controls/Top Techniques

Access Control	Awareness and Training	Audit and Accountability	Assessment, Authorization, and Monitoring	Configuration Management	Contingency Planning	Identification and Authentication	Incident Response
AC-01	AT-01	AU-01	CA-01	CM-01	CP-01	IA-01	IR-01
AC-02	AT-02	AU-02	CA-02	CM-02	CP-02	IA-02	IR-02
AC-03	AT-03	AU-03	CA-03	CM-03	CP-03	IA-03	IR-03
AC-04	AT-04	AU-04	CA-04	CM-04	CP-04	IA-04	IR-04
AC-05	AT-05	AU-05	CA-05	CM-05	CP-05	IA-05	IR-05
AC-06	AT-06	AU-06	CA-06	CM-06	CP-06	IA-06	IR-06
AC-07		AU-07	CA-07	CM-07	CP-07	IA-07	IR-07
AC-08		AU-08	CA-08	CM-08	CP-08	IA-08	IR-08
AC-09		AU-09	CA-09	CM-09	CP-09	IA-09	IR-09
AC-10		AU-10		CM-10	CP-10	IA-10	IR-10
AC-11		AU-11		CM-11	CP-11	IA-11	
AC-12		AU-12		CM-12	CP-12	IA-12	
AC-13		AU-13		CM-13	CP-13		
AC-14		AU-14		CM-14			
AC-15		AU-15					
AC-16		AU-16					
AC-17							
AC-18							
AC-19							
AC-20							
AC-21							
AC-22							

Controls Evaluation



Assessment, Authorization, and Monitoring	Configuration Management	Contingency Planning	Identification and Authentication	Risk Assessment	System and Services Acquisition	System and Communications Protection	System and Information Integrity	Supply Chain Risk Management
CA-1	CM-1	CP-1	IA-1	RA-1	SA-1	SC-1	SI-1	SR-1
! CA-2	! CM-2	! CP-2	! IA-2	RA-2	SA-2	! SC-2	! SI-2	SR-2
! CA-3	! CM-3	CP-3	IA-3	RA-3	! SA-3	! SC-3	! SI-3	SR-3
CA-4	CM-4	CP-4	! IA-4	RA-4	! SA-4	SC-4	! SI-4	! SR-4
CA-5	! CM-5	CP-5	! IA-5	! RA-5	SA-5	SC-5	SI-5	! SR-5
CA-6	! CM-6	! CP-6	! IA-6	RA-6	SA-6	SC-6	SI-6	! SR-6
! CA-7	! CM-7	! CP-7	IA-7	RA-7	SA-7	! SC-7	! SI-7	SR-7
! CA-8	! CM-8	CP-8	! IA-8	RA-8	! SA-8	SC-8	SI-8	SR-8
CA-9	CM-9	! CP-9	! IA-9	RA-9	SA-9	SC-9	SI-9	SR-9
	CM-10	! CP-10	IA-10	! RA-10	! SA-10	SC-10	! SI-10	SR-10
	! CM-11	CP-11	IA-11		! SA-11	SC-11	SI-11	! SR-11
	CM-12	CP-12	! IA-12		SA-12	SC-12	SI-12	SR-12
	CM-13	CP-13			SA-13	SC-13	SI-13	
	CM-14				SA-14	SC-14	SI-14	
					! SA-15	SC-15	SI-15	
					! SA-16	SC-16	! SI-16	
					! SA-17	SC-17	SI-17	
					SA-18	! SC-18	SI-18	
					SA-19	SC-19	SI-19	

Wrapping Up

- Testing is a very effective way to evaluate security controls
- Purple teaming yields better results than red/blue teaming
- Bringing together diverse teams is a much better way to drive changes the organization
- Constantly reavaluate the threat scenario and your defense capabilites
  - Adapt accordingly

Next Steps

- Find your Top Techniques
  - Start with the calculator's defaults
- Understand the methodologies
  - Tailor it to your environment
- Develop risk capabilities on your tech team, and tech capabilities on your risk team

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

Contact information:

Carlos Gonçalves – cgoncalves@bb.com.br
Linkedin: @carlosecg
Mastodon: @cgoncalves@infosec.exchange